Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1724 07/03/15

~ PS4 Dominating Europe! ~ Planet Coaster Readies ~ Xbox Gamescom!

-* OPM Chief Rebuffs Lawmakers! *-
-* US, Brit Spies Targeted AV Companies *-
-* China Denounces Hacking Accusation, Absurd *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

Happy Independence Day, America! Yes, the 4th of July holiday weekend is upon us already! While we remember this date for independence, most of us will be celebrating with cookouts and fireworks. One of my dogs will likely be hunkered down in the closet soon after dusk - he hates the sound of fireworks!

For us personally, we're going to go the seafood route on Saturday: lobster, steamers and shrimp. However, I'll be sure to have a nice steak ready for the grill on Sunday! And yes, the beer is chilling in the fridge!

Oh, before I forget, apologies for yet another "missed" issue last week. There just wasn't enough material to put together a full issue, so I opted to hold off and make sure we had plenty for the next issue. You won't be disappointed, other than having one less issue to pore over.

Enjoy the 4th, and be safe!

Until next time...

=~=~=~=

NetBSD/Atari 7.0_RC1 Available

Hi,

It looks the official announcement is not yet, but
NetBSD 7.0_RC1 binaries are already available on ftp:
ftp://ftp.NetBSD.org/pub/NetBSD/NetBSD-7.0_RC1/atari/

If someone can try it on the real machine, it would be great :-)

(I have too many other machines to be tested
which have less users than atari..)

Posting dmesg to NYC*BUG dmesgd page is also interesting:
http://dmesgd.nycbug.org/index.cgi

Izumi Tsutsui

=~=~=~=

->In This Week's Gaming Section - Xbox Gamescom Briefing Next Month!
PS4 Is Dominating Europe!
Remembering Nuon!
And much more!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!

Xbox Gamescom Briefing Includes Exclusives Missing from E3

With E3 now over, Microsoft is looking ahead to the summer's next big industry event, Gamescom, which is open to the public and runs from August 5-9 in Cologne, Germany.

The company has officially announced plans for the show, confirming that its briefing will take place on August 4 at 7 a.m. PDT / 10 a.m. EDT / 4 p.m. CET.
Microsoft says it will use the briefing to highlight the "greatest games lineup in Xbox history," including Xbox One exclusives like Scalebound, Quantum Break, and Crackdown.

These games were nowhere to be seen at E3 earlier this month.

For its part, Microsoft said previously that it was purposefully holding back some games and announcements from its E3 showing to use for Gamescom. Microsoft has major plans for the event, as the company will have as much new content to show there as they did at E3.

Microsoft's Gamescom briefing will be streamed live. GameSpot will have all the news for you as it's announced.

If you're attending the show itself--which is open to the public--you can visit the Xbox booth to play upcoming Xbox games like Halo 5: Guardians, Forza Motorsport 6, and Rise of the Tomb Raider. Microsoft is also holding an "Xbox FanFest" this year at Gamescom, with more details about this promotion scheduled to be announced later.

Sony is not holding a Gamescom briefing this year, instead choosing to make announcements at Paris Games Week in October.

Sony: PS4 Is Dominating Europe, No Plans for Price Cut

The PlayStation 4 is far and away the leading current-generation console in Europe, Sony Europe president Jim Ryan has revealed in a new interview. Speaking with VG247, Ryan claimed the PS4 is currently enjoying nothing less than 70 percent marketshare in every European country.

"We have a very significant market leadership," the executive explained. "We have market leadership in every country in Europe, and have very significant market leadership in continental Europe. Extremely significant. I don't think marketshare's any less than 70 percent, and frequently greater than 90 percent in continental Europe."

Also in the interview, Ryan explained that the PS4 is still seeing "very considerable" momentum at its current price point. As such, he said Sony has no immediate plans to cut the price of the console.

"We're happy with the price and we're happy with the value proposition," Ryan said. "We'll leave it where it is for now."

Globally, the PS4 has sold more than 22.3 million units as of March 31.

Planet Coaster Is Getting Ready for A Big Ride

Frontier Developments announced Planet Coaster at E3 last week. Apart from a trailer screened at the PC Gaming Show, very little detail about the game was announced.

Polygon caught up with David Braben at E3 to talk about the new game, which he described as an attempt to revive a "long-dead genre."

"We're revisiting every aspect of that genre from scratch and doing it properly," he said. "We've got so many fans of these coaster park simulation games. We know what works very well and what doesn't."

Frontier developed RollerCoaster Tycoon 3, released back in 2004 by Atari. Braben said that game has sold "more than 10 million copies," partly because it was built to anticipate advances in PC gaming technology.

"When we did RollerCoaster Tycoon 3, all those years ago, we worked really hard to make it the best game. It stood out from others at the time. We were even criticized for some of the things we did on the graphics. We pushed those out. We supported pixel shaders. We supported reflective water.

"For that reason, the game continued to sell well. It hit number one on the charts nearly 10 years after it was released. It's still the de facto 'coaster game, all those years later, despite a lot of people trying to do them."

The new game is being built on the company's Cobra engine, which was used on RollerCoaster Tycoon 3. "We can do so much more now and we can do it so much better," said Braben. "We've learned a lot since then. Cobra now is so much more advanced than it was when shipped Tycoon 3 in 2004."

Given Braben's history of embracing technology and the fact that Frontier's space-trading game Elite: Dangerous is on Oculus Rift, it

seems likely that Planet Coaster will feature VR rollercoaster rides, though Frontier won’t talk details yet.

"You’re building a theme park," said Braben. "You’re keeping people happy. When you’re setting all the rules of that, we’ll make it work in a way that is as intuitive as possible. It will feel like something new, something fresh. We’re looking at how we can add all these features and make them adorable, how to make them lovely. Hopefully you’ll see from the trailer for Planet Coaster that there’s a lot love there. There’s a lot of beauty, a lot of emotion."

Planet Coaster is coming out for PC in 2016.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

Last of Atari Games To Go Up for Auction on eBay

The last batch of Atari game cartridges dug up in an Alamogordo landfill will be going up for auction.

The Alamogordo Daily News reports that 150 remaining games and they will be put on eBay in 30-40 increments until the last one is sold.

The games up for bid include Warlords, Asteroids and Super Breakout. Joe Lewandowski, a consultant for the film companies that documented the dig, says some E.T. The Extra Terrestrial cartridges and other titles will be kept off until the very end.

More than 700 games have been sold around the U.S. and abroad, bringing in thousands of dollars to Alamogordo.

One of the E.T. game cartridges was added to the Smithsonian s video game history collection.

Remembering Nuon, The Gaming Chip That Nearly Changed The World But Didn t

Behold, a chip that almost changed everything.

In the Wild West of Silicon Valley startups of the late 1990s, one little company looked like it might accomplish something incredible. VM Labs had some of the best engineering talent in the world, an explosive mix of bright young minds with burning ambition and experienced old hands who once held key positions in companies such as Atari, Sony, and Sega. Their business revolved around a little chunk of silicon codenamed "Project X. Later, they officially named their dream chip the Nuon. VM Labs believed it might change the world.

The Nuon was so much more than a chip it was a complete multimedia platform with an operating system and a Web browser. It would turn any DVD player in the world into a game console. And at a time when DVD looked like it would soon be everywhere, the Nuon could be right there with it.

VM Labs' goal for the Nuon was huge but straightforward: total market penetration. The company wanted a Nuon chip inside every DVD player. For a time, it actually seemed attainable.

Yet Nuon failed spectacularly. After quietly gathering hype for years at consumer electronics shows and in magazines such as Wired and Next Generation, the Nuon launched more than a year behind schedule in the middle of 2000 the same year that Sony's much-hyped DVD-compatible PlayStation 2 game console debuted. The Nuon was included in only two of the dozens of DVD player models released that year.

Nuon reviews were positive, but a raft of factors poor timing and diminishing finances chief among them combined to sideline the platform, sending its creator into bankruptcy before it could gather much steam. The chip that nearly changed the world didn't, and the company that made it disappeared. But Nuon came so very close to transforming home entertainment.

Cast your mind back to November 1994. Games were mostly sold on cartridges, while movies came on VHS tapes. Somewhere in America, a Boyz II Men slow jam played on the radio as the Moving Picture Experts Group (MPEG) announced what would become the de facto standard in digital video compression: MPEG-2. MPEG-2 hardly sparked fireworks, but, in the years that followed, it quietly achieved what its predecessor MPEG-1 could not making analog video obsolete and finally killing off VHS. MPEG-2 did this in large part because of a delivery technology under development at the same time: DVD.

VM Labs founder Richard Miller, a British ex-pat, was working at Atari Corporation when he heard the news about MPEG-2. Miller had been heavily involved in the creation of Atari's 64-bit Jaguar game console, which was already petering out after just a year on the market. "We were very proud of it," he said in a recent interview. "But it did not succeed because of the lack of content and a chicken and egg issue of getting mainstream developers to support it and having to discount the hardware and all these kinds of things."

"I was thinking there must be a better way," he continued. "I saw DVD happening and thought DVD could be a really good vehicle for launching a new game console."

Miller quit Atari and sold his house, and he then started VM Labs in a spare bedroom at the beginning of 1995. It was his second company. His first built the world's first parallel-processing graphics workstation, which was licensed to Atari but failed commercially. Miller had also, earlier in his career, been instrumental in developing an early, A4-sized laptop computer called the Z88.

Miller knew how to design systems and build platforms. He realized that it wouldn't cost much to install a smarter, more powerful processor in place of a DVD player's basic video decoder. The idea was a processor that could handle games, perhaps things beyond games. "I kind of hoped that it would be a real computing platform, much as the Atari ST had been a platform that was used for games as well," Miller said.

Five people invested $200,000 in the company (the first of whom was Miller’s landlord), which was enough for Miller to rent office space and hire a few people in April 1995. He also brought in lawyer Nicholas Lefevre, whose biggest claim to fame is being the first to file an antitrust lawsuit against Microsoft (back in 1983). Lefevre had briefly worked with Miller at Atari before leaving to form his own private practice.

Lefevre helped round out the business plan. VM Labs would leverage the analog to digital shift by building a platform around its chip and establishing a two-tiered licensing model. The chip would be licensed to manufacturers, while the software technology would be licensed to content creators and publishers. First the team needed to build everything chip and tools from scratch.

Miller used his business plan to chase down more funding. "Atari had built relationships at Motorola," Miller said. "So I got those guys in very early on and they jumped in with both feet and said, ’Hey, we’ll make your chips for you.’"

The next step was to find an electronics company that would put the chips in their products. Miller’s first thought was of DVD’s principal creators, Toshiba engineers Hisashi Yamada and Koji Hase. "I actually just picked up the phone, called Toshiba in Tokyo, and asked for those guys by name," Miller said. "I [eventually] got through to someone who worked directly for these two guys, and we had a couple more calls. He said, ’Why don’t you come out to Japan?’"

Miller flew over to Tokyo and built a friendship with the engineers. Still, even with this promising start, he needed help. He had limited business experience and knew little of Japanese culture. Luckily, one of his engineers knew somebody who did a guy called Bharath Ram, who had just moved on from a successful business development stint in the encryption market with RSA Security.

"Bharath came in and really cultivated that relationship [with Toshiba] because he speaks fluent Japanese," said Miller. "You wouldn’t be able to tell he wasn’t Japanese."

Ram bridged the divide between American and Japanese business cultures, which was important because Nuon’s success depended on support from the "tier one" Japanese electronics companies principally, Matsushita (now known globally as Panasonic), Toshiba, and Sony.

Early meetings with Toshiba went well. The multi-core Nuon processor that VM Labs was developing packed a big punch in terms of graphics and performance, and the Toshiba representatives were impressed. As early as 1996, the in-development chip could already demonstrate basic ray tracing, and it had a Mandelbrot set (a complex kind of fractal) browser that could produce several frames per second in real time. "Nothing else would do that at the time," former VM Labs Senior Software Engineer Ken Rose said.

Ahead of its time in architecture as well as concept, Nuon featured four fully programmable, very long instruction word (VLIW) processor cores or "Media Processor Elements" running at 108 MHz each. It was a parallel processor not unlike the PlayStation 3 that came several years later. Nuon’s design suited its function. The MPEs were fast at exactly the kinds of calculations needed for interactive video and games, and they could also be generalized to other media-rich applications such as Web browsing,

interactive audio, and the sorts of reference and educational multimedia that was all the rage in the 1990s. Being a programmable processor, Nuon could gain support for new media codecs from a simple firmware update. And being a specialized VLIW solution, Nuon hardware engineer John Mathieson explained, the chip could be dramatically more efficient than software solutions built with the general purpose processors found in personal computers.

It took almost a year of alcohol- and sushi-filled meetings for VM Labs and Toshiba to hammer out an agreement, with Miller flying tirelessly back and forth to work with both his engineers and Toshiba management.

"Now, when we're doing this, here is where the kabuki starts," recalls Ram.

DVD players in the US needed to be in Circuit City or they would struggle to sell in significant volumes. But Circuit City had just partnered with Thomson on the Digital Video Express format, known as DIVX for short (this is not to be confused with the completely different, unrelated video codec, DivX, which came later and is still in use). DIVX was basically DVD with some tweaks that allowed discs to have time limitations; you had to pay an additional fee to get another two days of viewing or to get an unlimited number of viewings.

Circuit City still stocked DVD players, but it tried to push customers to DIVX. "At that point Thomson had put a gun at our head and said, 'Hey, would you guys support DIVX?'" Ram said. "Here was a startup with barely 30 people having to make a momentous decision which way do you want to go? There was no way in hell our company would have been able to support two competing formats, not with the kind of funding and resourcing that we were at."

VM Labs chose to stick it out with Toshiba. By the end of 1999, DIVX was dead killed in part because its performance was inferior to DVD and in part because Hollywood was weary of a Betamax versus VHS-style war and chose a side early.

The kabuki didn't end there. Matsushita remained reluctant to adopt the VM Labs chip, so Sony wouldn't budge. And without Thomson US, which pulled out after the DIVX snub, Matsushita wouldn't need to worry about being the odd duck out in Circuit City. The company could continue to play hardball.

"We were trying to convince these guys that we're not a chip company," Ram said. "We're really a platform. What we're going to do is turn your DVD machine into something that's far more strategic. We were trying to sell a vision that the Japanese did not appreciate or share."

They got the vision later, when Blu-ray and HD DVD came around in the mid-2000s. "But it was after I think they read the tea leaves in the market," Ram said. "Unfortunately this was in 1998, when the DVD format had just come out. The fact that we were able to stretch our imagination and say this is where the markets will go at some point in the future was something that their incremental minds could not appreciate. Not every company has a Steve Jobs at its helm who's able to sway its audience. Here was a guy a self-deprecating Brit engineer trying to convince the hardened Japanese businessmen that they ought to place their bets on this product."

The Japanese manufacturers were not comfortable with firmware updates. "They didn't want the computer experience to be transferred to consumer electronics," Ram said. And that extended not just to updates but also to

error handling "If something goes wrong there’s got to be a way to flash the firmware quickly and restore it to the last best-known state" and startup times. Toshiba expected things to just work.

"I think for the Japanese it was really kind of welcome to the new world," Ram said. "Software changes the way you need to think, so that was the other big revelation for them. And I was right there sitting between these two cultures.

"You would have these conversations where the Japanese guy would be basically swearing at us and I’d have to figure out a way to translate that to my team. But then when they switch to English they would say it in a very polite way. They’d say, ’Please, Mr. Miller, would you please ensure that you’re doing ABC?’ It would be with a please and a very polite English expression. Then they’d turn to me in Japanese and say, ’Isn’t this guy an idiot for not having done this to the platform? Is this what you’d expect in Japan? If I had a supplier I’d be basically throwing him down the next biggest bridge of Shinjuku [a busy business hub area in Tokyo].’"

Ram had better luck with Samsung. The Korean electronics giant bought in aggressively, demanding that it be first to market with a Nuon-enhanced DVD player. "One of the concerns that Toshiba had that they kept hammering on me," Ram said, "was, ’Look, if you guys launch with Samsung, you’re going to spoil the image on this platform because these guys are not known for the quality or vision that we are planning to deliver on it.’"

Meanwhile, Sony made a strategic shift. "Ken Kuturagi [PlayStation’s chief architect] looked at what Toshiba was going to do," Ram said. "He looked at what Samsung had announced. And I think there was a big fear within Sony that Nuon would basically pull the rug out from under Sony."

Kuturagi decreed that the PlayStation 2 would have DVD playback functionality. Sony’s home entertainment division was furious and fought to stop the move for fear that it could cannibalize sales of Sony-branded DVD players, but they were powerless to stop Kuturagi and his growing computer entertainment division.

"There was also a bit of panic within the Toshiba camp because they wanted to make sure that the launch Toshiba [Nuon] DVD player would have at least a few titles, both game as well as movie titles," Ram said. "Here’s a very classic Japanese response this is a culture where you don’t want to take your competitor head on. It’s like basically let’s all figure out a way to survive in the marketplace." Sony could have its hardcore games, essentially, and Nuon at least from Toshiba’s perspective could push more for a casual audience.

The original Nuon vision didn’t extend to interactive movie features such as zooming and panning or highlighting an object in a scene to trigger bonus content. But these sorts of features nevertheless became key to the platform strategy. To help woo Hollywood studios, Miller hired Sony Pictures veteran Paul Culberg and another of his former Atari colleagues James Grunke in 1999.

"They had a tough time," Miller said. VM Labs was small, maybe 50 people by then, and almost completely unknown. Culberg had the contacts and pull to get meetings and form relationships between VM Labs and the big studios. But while Hollywood liked the technology, it was hesitant to produce Nuon content. "The studios were pretty clear," Ram said. "’We want more manufacturers. We want to see more units. We need to see a lot more

in the retail [chains].’"

Miller recalled the Hollywood outreach efforts as an expensive mistake on his part.

"I think in hindsight the interactive movie features were weak," he said. "I mean, from a consumer perspective I wouldn’t buy a player for that." Nuon’s strength lay elsewhere, and as exciting as the interactive movies tech was to everyone at the company, Miller now believes that the initiative stretched his company too thin and strained finances.

Good decision or not, VM Labs did manage to get multiple studios on board. CBS released a Nuon-enhanced edition of comedy flick Bedazzled, MGM put out its sci-fi oddity The Adventures Of Buckaroo Banzai, and 20th Century Fox sold Dr. Dolittle 2 and Tim Burton’s Planet of the Apes remake in Nuon special editions.

But other efforts to build partnerships for entertainment software faltered. Atari veteran Bill Rehbock spearheaded efforts to broker agreements with big-name game companies. Like Hollywood, the big software publishers held back from significant commitments. VM Labs senior account manager for third-party development and director of licensing Scott Hunter recalls that publishers were reluctant "to hook their horse to ’potential.’" A few ports were announced for games such as Myst and Madden NFL, but no big hitters made it to market.

"It was really the smaller developers who jumped on board early and started playing with the development system," Hunter said. The caveats with these smaller developers were two-fold: VM Labs would have to self-publish the games, which incurred yet more expense for the startup, and the titles had little name recognition to sell the system to gamers.

Nuon’s biggest game became Jeff Minter’s Tempest 3000, which followed up Minter’s cult hit Jaguar (and later PC, Saturn, and PlayStation) remake of 1981 arcade classic Tempest with even more insane real-time graphics effects.

Tony Takoushi, a former games journalist and development/publishing veteran (he worked at Sega from 1988 to ’94), was itching to do something totally new and original. Minter, a friend, suggested he pitch the idea to VM Labs, which greenlit development on Takoushi’s Freefall 3050 AD. It was a strange and disorienting action game about a cop in a world where people lived in the sky.

Takoushi recalls that development was something of a nightmare because his team started making Freefall before VM Labs finished writing the software tools. "We had to switch the ’lead’ CPU in the last few weeks from one of the four [MPE] processors to processor ’zero,’" he said. "This wasn’t too bad for us... however, for Jeff’s Tempest it was massive change as he wrote the game in assembly language and it entailed what I believe was a massive rework."

More concerning for game developers was that as launch day neared, marketing plans disappeared. Without big marketing or hype behind them, Takoushi and other Nuon developers struggled to get attention from the press (though those who did try Freefall praised its originality). Sales were distinctly low fewer than 10,000 units for Freefall.

Kevin Manne, creator of the Nuon-Dome website, remembers this time well. He was one of the Nuon’s super fans, a Jaguar diehard who followed Miller

and company from Atari and eagerly bought a Nuon for Tempest and Merlin Racing (a sequel to a Diddy Kong Racing-like Jaguar game called Atari Karts). "Over time it became that if you wanted to buy a Nuon game you had to go digging through the DVDs to try and find it," he said. "It just got shoved in there because some employee didn’t realize that it was a video game and not a regular DVD."

From a gamer’s perspective, Nuon was a tough sell. Its games lineup numbered just eight titles a year after launch. As former VM Labs engineer Scott Cartier pointed out, "It also didn’t help that our graphics capabilities were comparable with PS1 and N64 when the console market had moved on to Dreamcast."

Mass production took a while to get rolling. Samsung’s first Nuon-enhanced DVD player started trickling out around the end of May 2000, soon followed by Toshiba’s model and a full retail release at a price of around $300 to $350. Set-top boxes with Nuon inside started to proliferate more widely at the same time.

Again, Nuon was well received, though it was hardly the revelation it should have been. The hype had moved to other things, the launch titles were running late, and VM Labs was almost out of money.

"The launch experience was like riding a Mach 5 aircraft with all kinds of twists and rolls," said Ram. "And imagine you’re not the guy piloting the plane; you’re sitting in the back with your helmet on and wondering if you’re going to make it through."

"By 2001, I was spending literally 100 percent of my time on funding," said Miller. The company needed cash to stay afloat until the Nuon revenues started to come in, which would take a while because of the licensing model used.

VM Labs was "close" to profitability. Toshiba and Samsung had entered mass production and around a dozen software titles were out. A few more months and the company might have been able to turn a corner. But close wasn’t good enough. "We were just out of cash," Miller said. "We couldn’t pay people and it wasn’t right to have people in the building." Many VM Labs employees continued showing up to work, still believing in the vision. "We had to kind of push people away because nobody wanted to accept it," Miller said.

There was no lifeline because the financial markets had flatlined. The dot-com bust was compounded by the September 11, 2001 terrorist attacks. VM Labs had been trying to close a new funding round and was in talks to be acquired when the tragic incident happened. "After 9/11, the investors literally didn’t pick up the phone," Miller said.

To save the company from being picked apart by "vultures," Lefevre soon resigned and got together the money and paperwork to put VM Labs into Chapter 11 bankruptcy. Some of the technology was sold to Pixelworks, where Miller now works, while the rest went to Genesis Microchip. The 50 or so employees that VM Labs still had followed to Genesis.

Genesis Microchip briefly kept the Nuon rolling along as before. Efforts to get emerging low-cost Chinese manufacturers on board failed, and a deal fell through with Disney in 2003 to have Nuon incorporated into a DVD player for tween and teen audiences. Genesis then cut its losses and dropped the platform part of Nuon.

Nuon stands today as one of the greatest might-have-been computing and entertainment platforms. The Nuon team members interviewed for this story all pointed to funding they really needed $60 million, not $30 million over the life of VM Labs and launch delays as the biggest culprits in Nuon’s failure. The basic business model works, but it needs big money or positive cashflow to get rolling.

"It took a company like Sony to do it with the PlayStation," Miller said. "You look at how much money went into the PlayStation, numbers bandied around of a billion dollars that they were in the red before they started to get positive."

But VM Labs had more going against it than the size of its bankroll. "The reviews saying someday all DVD players will rock this hard were all well and good," said Lefevre. "But when consumers were walking into Best Buy and all they saw was a wall of DVD players and prices nobody willing or able to demonstrate the features the price point was not competitive." More trouble was just around the corner too, as prices dropped rapidly on DVD players when the Chinese manufacturers took over the market from around 2003 onward.

An earlier release (say, late 1998) would have put Nuon in a much stronger position, clear of more powerful game consoles such as the Dreamcast and PlayStation 2 and well positioned to ride the DVD and video on demand waves. "Digital video was I think an ideal Trojan Horse," said Lefevre. "Ours was one of the great potential times to get something that would be really pervasive in homes."

Like many technologies that fail, Nuon was a victim of its time. Hunter succinctly describes what was perhaps its biggest problem, saying, "At that time, a game machine was a game machine and a DVD player was a DVD player." Nuon’s vision was somehow too big, too grand for its era in home entertainment.

Now, as Mathieson points out, "There are too many entrenched players with too much to lose by letting any one entity get too powerful." But for a brief moment, a few years around the turn of the millennium, a company that for most of its life had fewer than 30 people very nearly changed the world with a simple idea and a clever bit of technology.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

OPM Chief Rebuffs Lawmakers on Scope of Cyber Breach

The director of the Office of Personnel Management refused on Wednesday to estimate how many millions of Americans were affected by recent attacks on her agency’s computers and rejected as premature reports 18 million were compromised.

Under blistering attack from lawmakers exasperated by unanswered questions about the massive cybersecurity breach, OPM Director Katherine Archuleta conceded the number of people whose data was hacked could increase from initial reports.

OPM said this month it was victim of a cyber attack involving personnel data on 4.2 million current and former federal employees. Another attack targeted information of millions more Americans who applied for security clearances. Some media reports said 18 million were affected in that attack.

"It is my understanding that the 18 million refers to a preliminary, unverified and approximate number of unique Social Security numbers in the background investigations data," Archuleta said at a House of Representatives hearing.

"It is a number that I am not comfortable with at this time."

In her second appearance in as many weeks before the Oversight and Government Reform Committee, Archuleta defended her agency's response to the intrusions. The hearing, which lasted four hours, was the second of at least three this week on the OPM breaches.

Senate Majority Leader Mitch McConnell criticized her Tuesday testimony as "world-class buck-passing" and said there was a "management problem" at the agency.

Lawmakers have criticized the OPM response to questions about the hacking sluggish and incomplete. Some called on the director, who has been in her job less than two years, to resign or at least take the blame for the sweeping breaches, which U.S. authorities suspect are the work of Chinese hackers.

U.S. Representative Jason Chaffetz, the Republican committee chairman, exasperated by Archuleta's refusal to provide numbers, asked whether all 32 million current and former federal workers in its database could have been compromised.

But Archuleta steadfastly refused to give an estimate.

"As much as I want to have all the answers today, I do not want to be in a position of providing you and the affected individuals with potentially inaccurate data," she said.

Archuleta said the second breach is still being investigated and that the number of people affected by that data intrusion "may well increase from these initial reports."

Lawmakers also criticized agency contractors, whose practices have been cited as a factor in the successful hacks.

Representative Elijah Cummings, the senior Democrat on the panel, singled out contractor KeyPoint Government Solutions for being the weak link that allowed hackers into the OPM system. Lawmakers said they were frustrated with a lack of information from that company's chief executive, Eric Hess.

"I find myself utterly dissatisfied with the explanations we've heard today," said panel Democrat Matt Cartwright.

China Denounces US Hacking Accusation As ’Absurd’

Beijing on Friday denounced as "absurd logic" accusations by the head of US intelligence that China was the main suspect in a massive hack of government data files in Washington.

James Clapper, US director of national intelligence, said China was "the leading suspect" behind the breach affecting personal data of millions of US government employees, which was revealed earlier this month.

Chinese foreign ministry spokesman Lu Kang responded: "We have noticed that the US is still investigating, but feels that China is responsible. This is absurd logic.

"We understand this as showing the US has adopted the presumption of guilt rather than the presumption of innocence," he added at a regular briefing.

The US has in recent years blamed several hacks on Beijing, including some it says were carried out by members of the Chinese military.

Cybersecurity specialists said the breach of data on at least four million current and former federal employees appeared to be part of an effort to build a database for espionage.

Soon after the breach was made public, US officials told media they believed China was involved. Beijing rebuffed the claims as "unscientific".

The US Office of Personnel Management said that employees, retirees, contractors and job applicants may have had their personal information compromised in the breach.

Some reports have said the number affected may be 14 million or higher, after officials said the total was still being determined.

Facing an outcry from employees and lawmakers, the US administration has announced new steps to boost the security of its online records, including in some parts that still use decades-old technology.

US and British Spies Targeted Antivirus Companies

When the Russian security firm Kaspersky Lab disclosed recently that it had been hacked, it noted that the attackers, believed to be from Israel, had been in its network since sometime last year.

The company also said the attackers seemed intent on studying its antivirus software to find ways to subvert the software on customer machines and avoid detection.

Now newly published documents released by Edward Snowden show that the NSA and its British counterpart, GCHQ, were years ahead of Israel and had engaged in a systematic campaign to target not only Kaspersky software but the software of other antivirus and security firms as far back as 2008.

The documents, published today by The Intercept, don t describe actual computer breaches against the security firms, but instead depict a systematic campaign to reverse-engineer their software in order to uncover vulnerabilities that could help the spy agencies subvert it. The British spy agency regarded the Kaspersky software in particular as a hindrance to its hacking operations and sought a way to neutralize it.

Personal security products such as the Russian anti-virus software Kaspersky continue to pose a challenge to GCHQ s CNE [Computer Network Exploitation] capability, reads one of the documents, and SRE [software reverse-engineering] is essential in order to be able to exploit such software and to prevent detection of our activities.

An NSA slide describing Project CAMBERDADA lists at least 23 antivirus and security firms that were in that spy agency s sights. They include the Finnish antivirus firm F-Secure, the Slovakian firm Eset, Avast software from the Czech Republic. and Bit-Defender from Romania. Notably missing from the list are the American anti-virus firms Symantec and McAfee as well as the UK-based firm Sophos.

But antivirus wasn t the only target of the two spy agencies. They also targeted their reverse-engineering skills against CheckPoint, an Israeli maker of firewall software, as well as commercial encryption programs and software underpinning the online bulletin boards of numerous companies. GCHQ, for example, reverse-engineered both the CrypticDisk program made by Exlade and the eDataSecurity system from Acer. The spy agency also targeted web forum systems like vBulletin and Invision Power Board used by Sony Pictures, Electronic Arts, NBC Universal and others as well as CPanel, a software used by GoDaddy for configuring its servers, and PostfixAdmin, for managing the Postfix email server software But that s not all. GCHQ reverse-engineerred Cisco routers, too, which allowed the agency s spies to access almost any user of the internet inside Pakistan and to re-route selective traffic straight into the mouth of GCHQ s collection systems.

To obtain legal cover for all this activity, the GCHQ sought and obtained warrants granting permission to reverse-engineer the software. The warrants, issued by the UK Foreign Secretary under the UK s Intelligence Services Act 1994 Section 5, gave the spy agency permission to modify commercially available software to enable intercept, decryption and other related tasks. One of the warrants, used to reverse-engineer Kaspersky software, was valid for six months from July 7, 2008 to January 7, 2009, after which the agency sought to renew it.

Without a warrant, the agency feared it would be in breach of Kaspersky s customer licensing agreement or violate its copyright. Software makers often embed protection mechanisms in their programs to thwart reverse-engineering and copying of their programs and include language in their licensing agreements prohibiting such activity.

Reverse engineering of commercial products needs to be warranted in order to be lawful, one GCHQ agency memo noted. There is a risk that in the unlikely event of a challenge by the copyright owner or licensor, the courts would, in the absence of a legal authorisation, hold that such activity was unlawful[ ]

But, according to The Intercept, the warrant itself was on shaky legal grounds since the Intelligence Services Act, Section 5, references interference with property and wireless telegraphy by intelligence agencies but does not mention intellectual property. Its use to authorize

copyright infringement is novel, to say the least.

Earlier this month, Kaspersky disclosed that it had been hacked last year by members of the infamous Stuxnet and Duqu gangs. The intruders remained entrenched in the security firm s networks for months siphoning intelligence about nation-state attacks the company is investigating and studying how Kaspersky s detection software works so they could devise ways to subvert it on customer machines. Kaspersky claims to have more than 400 million users worldwide.

The attackers were also interested in the Kaspersky Security Network, an opt-in system that gathers data from customer machines about new threats infecting them. Any time Kaspersky s antivirus and other security software detects a new infection on the machine of a customer who has opted-in to the program, or encounters a suspicious file, data gets sent automatically to Kaspersky s servers so the company s algorithms and analysts can study and track emerging and existing threats. The company uses KSN to create maps outlining the geographical reach of various threats and is an important tool for tracking nation-state attacks from agencies like the NSA and GCHQ.

The newly published NSA documents describe a different method for gaining intelligence about Kaspersky and its customers. The spy agencies apparently monitored email traffic coming to Kaspersky and other antivirus companies from their customers in order to uncover reports about new malware attacks. The spy agencies would then examine the malware sent by these customers and determine if it had use to them. A 2010 presentation indicates that the NSA s signals intelligence would pick out for analysis about ten new potentially malicious files per day out of the hundreds of thousands that came into Kaspersky s network each day. NSA analysts would then check the malicious files against Kaspersky s antivirus software to make sure they weren t being detected by the software yet, then the NSA s hackers would repurpose the malware for their own use, checking periodically to determine when Kaspersky had added detection for the malware to its anti-virus software.

The Internet Is Officially Too Big

The Internet has (sort of) run out of space.

The regional organization tasked with assigning IP addresses in North America, the American Registry for Internet Numbers (ARIN), is now wait-listing all applicants because it has almost exhausted its supply of IP addresses under the current protocol.

IP addresses are the numerical labels that identify any device connected to the Internet. These addresses enable smartphones, tablets, PCs and servers to find and communicate with one another. Each IP address is a unique label that provides a destination for information as it travels through the Internet.

Under the current protocol, Internet protocol version 4 (IPv4), addresses are designated by four series of numbers ranging from 0 to 255, like 69.171.224.0. But this protocol has been in use since the early days of the Internet, and almost all of the 4.3 billion possible labels of IPv4 are already in use meaning the Internet has essentially run out of real estate.

"Within three to four weeks, we will hit the point where there is no inventory," said John Curran, president and CEO of ARIN. The group announced the wait-list policy on Wednesday.

But this is more of a milestone for the Internet than a death sentence.

The imminent exhaustion of available of addresses under IPv4 was announced last year by the Internet Corporation for Assigned Names and Numbers (ICANN), the international organization that allocates addresses to regional registry groups like ARIN. And a new protocol that was developed in the 1990s, Internet protocol version 6 (IPv6), has already been deployed in response.

While the current protocol consists of only four groups of numbers, IPv6 consists of eight groups of both letters and numbers like 2a03:2880:f022:6:face:b00c:0:2 (the IPv6 address for Facebook's servers). It provides roughly 340 trillion trillion trillion (or 340-undecillion) unique combinations, an almost limitless number of addresses.

"Realistically, IPv4 cannot provide the Internet that we need and that everyone wants to have," said Curran, who points to the fact that IPv4 could not even support a world where all 7 billion people had just one device. "We are currently engaged in an extremely large tech conversion effort on a global scale for the largest technological system on the planet."

The deployment of IPv6 means that almost anything on the planet could connect to the Internet, paving the way for smart appliances, fabrics and bigger smart grids. And according to Curran, the new protocol is not only faster and more direct, but consumers will barely notice the transition.

IPv6 is already installed in most devices, and most websites have made themselves accessible through IPv6, but service providers have been slow to adopt the new protocol. According to Google, which collects statistics about IPv6 adoption, only 21% of all Internet traffic in the U.S. uses IPv6 and the numbers are even lower worldwide.

According to Curran, the Internet is undergoing a necessary evolution, and Internet service providers need to be prepared or the exponential growth of the information super highway will screech to a halt.

Major Internet Providers Slowing Traffic Speeds for Thousands Across US

Major internet providers, including AT&T, Time Warner and Verizon, are slowing data from popular websites to thousands of US businesses and residential customers in dozens of cities across the country, according to a study released on Monday.

The study, conducted by internet activists BattlefortheNet, looked at the results from 300,000 internet users and found significant degradations on the networks of the five largest internet service providers (ISPs), representing 75% of all wireline households across the US.

The findings come weeks after the Federal Communications Commission introduced new rules meant to protect net neutrality the principle that all data is equal online and keep ISPs from holding traffic speeds

for ransom.

Tim Karr of Free Press, one of the groups that makes up BattlefortheNet, said the finding show ISPs are not providing content to users at the speeds they re paying for.

For too long, internet access providers and their lobbyists have characterized net neutrality protections as a solution in search of a problem, said Karr. Data compiled using the Internet Health Test show us otherwise that there is widespread and systemic abuse across the network. The irony is that this trove of evidence is becoming public just as many in Congress are trying to strip away the open internet protections that would prevent such bad behavior.

The study, supported by the technologists at Open Technology Institute s M-Lab, examines the comparative speeds of Content Delivery Networks (CDNs), which shoulder some of the data load for popular websites. Any site that becomes popular enough has to pay a CDN to carry its content on a network of servers around the country (or the world) so that the material is close to the people who want to access it.

In Atlanta, for example, Comcast provided hourly median download speeds over a CDN called GTT of 21.4 megabits per second at 7pm throughout the month of May. AT&T provided speeds over the same network of of a megabit per second. When a network sends more than twice the traffic it receives, that network is required by AT&T to pay for the privilege. When quizzed about slow speeds on GTT, AT&T told Ars Technica earlier this year that it wouldn t upgrade capacity to a CDN that saw that much outgoing traffic until it saw some money from that network (as distinct from the money it sees from consumers).

AT&T has strongly opposed regulation of its agreements with the companies that directly provide connectivity between high-traffic internet users and their customers. Cogent, Level3 and others have petitioned the FCC to make free interconnection to CDNs a part of the conditions for the proposed merger between AT&T and DirecTV.

It would be unprecedented and unjustified to force AT&T to provide free backbone services to other backbone carriers and edge providers, as Cogent et al seek, said the company in a filing replying to the CDNs suggestion, part of a brief opposing the merger. Nor is there any basis for requiring AT&T to augment network capacity for free and without any limits. Opponents proposals would shift the costs of their services onto all AT&T subscribers, many of whom do not use Opponents services, and would harm consumers.

FCC chairman Tom Wheeler has taken an aggressive regulatory tack when it comes to mergers in the telecommunications sector. History proves that absent competition a predominant position in the market such as yours creates economic incentives to use that market power to protect your traditional business in a way that is ultimately harmful to consumers, he told industry leaders at the Internet and Television Expo last month.

The dispute over traffic speeds comes as the telecoms and cable industry readies legal challenges to the net neutrality rules. Most telecoms are content letting their lobbyists, notably trade associations Cellular Telecommunications Industry Association (CTIA) and USTelecom, sue the FCC over net neutrality rules, but AT&T has been one of the few companies to sue the FCC directly.

Twin Prodigies-turned-hackers Face Long Jail Yerms After Pleading Guilty

Twin brothers - one of whom set himself up for a visit from Homeland Security by boasting to a colleague at his new security job about jacking up the value of gift cards - have pleaded guilty to a series of schemes that involved stealing credit card information, breaking into State Department computers and filching data from a private company.

Muneeb and Sohaib Akhter, 23, of Springfield, Virginia, pleaded guilty on Friday in federal court in Alexandria, Virginia.

The brothers were once lauded as budding computer prodigies who, at the age of only 19, became the youngest graduates from George Mason University in 2011.

They went on to be rewarded a $200,000 research grant from the Defense Advanced Research Project Agency (DARPA).

Much was expected from them. Much was forthcoming.

But what came forth wasn’t good.

According to the US Attorney’s Office for the Eastern District of Virginia, the brothers have pleaded guilty to charges including conspiracy to commit wire fraud, conspiracy to access a protected computer without authorization, and conspiracy to access a government computer without authorization.

As well, Muneeb pleaded guilty to additional charges of accessing a protected computer without authorization, making a false statement, and obstructing justice.

According to the US Attorney’s Office, the defendants’ statements of facts detail one scheme that began around March 2014, when Muneeb broke into the website of a cosmetics company and stole thousands of customers’ credit card details and personal information.

The brothers used those details to buy flights and hotel reservations and to attend professional conferences.

Muneeb also passed the stolen information on to somebody he met on the Dark Net: a portion of the web that can only be accessed by tools like Tor or I2P. It uses encryption to preserve the anonymity and hide the location of the people who use it and the sites and services they use.

Because of that, it is a haven for thieves, child abuse imagery offenders, human traffickers, forgers and assassins, making it a fitting place for Muneeb to sell the stolen information to somebody who then cut him in on the profit.

Another scheme involved the brothers, along with co-conspirators, intruding into the US Department of State to get at passport and visa information.

Around February 2015, Sohaib Akhter used his contract position at the State Department to gain access to sensitive systems containing personally identifiable information (PII) of dozens of co-workers, acquaintances, one

former employee, and a federal law enforcement agent who was investigating Sohaib’s crimes.

Later, Sohaib came up with a plan to make sure he could always get access to the State Department systems: with Muneeb’s and unnamed co-conspirators’ help, he attempted to plug in an unspecified "electronic collection device" to enable them all to remotely access and collect data.

But it wasn’t to be: Sohaib muffed up the device installation, breaking it while trying to install the hardware behind a wall at a State Department building in Washington, D.C.

Another racket: around November 2013, Muneeb was working as a contractor for a private data aggregation company located in Rockville, Maryland.

He broke into the company’s database of federal contract information so that he and his brother could glean information to tailor successful bids in order to win contracts and clients for their own technology company.

Muneeb also inserted codes onto the company’s servers to rig an online contest, and to send more than 10,000 mass emails to students at George Mason University, also in the pursuit of contest votes.

Around October 2014, Muneeb lied about his computer-related crime history, as well as his employment history, on a government background nvestigation form.

His lies led to him successfully landing a job with a defense contractor.

Then, around March 2015, after his arrest and release pending trial, Muneeb obstructed justice by trying to whisk away a key co-conspirator so that investigators looking into their crimes couldn’t get at him.

That included driving the co-conspirator to the airport and purchasing a boarding pass to get him out of the country, to the Republic of Malta.

When the co-conspirator returned to the US, Muneeb encouraged him to lay low to avoid investigators.

The twins were indicted by a federal grand jury on 30 April 2015.

Muneeb faces a maximum penalty of 50 years in prison, and Sohaib is looking at a maximum of 30 years, though maximum sentences are rarely handed out.

Talent = squandered.

Hundreds of Dark Web Sites Cloned and "Booby Trapped"

The founder of one of the Dark Web’s fledgling search engines is warning Tor users about the presence of hundreds of fake and booby trapped .onion websites.

Sites with addresses that end in .onion are anonymous, Dark Web websites (properly called hidden services) that can only be accessed using the Tor browser.

The fake sites were discovered by Juha Nurmi, a founding member of the ahmia.fi project, an open source search engine that aims to search, index and catalogue all the content present on the Tor network.

Nurmi first noticed a fake of his own site before discovering that there are multiple clones of hundreds of other Dark Web sites, including a fake of the .onion version of the popular DuckDuckGo search engine.

Nurmi raised his concerns on Monday, on the Tor-Talk mailing list and published a full list of fake or booby trapped sites to Pastebin.

I noticed a while ago that there is a clone onion site for Ahmia. Now I realized that someone is actually generated similar onion domains to all popular onion sites and is re-writing some of the content.

In his post to the mailing list he claims that there are multiple copies of each target site with similar-looking addresses.

Tor sites are often found through directories rather than search engines and they have addresses that are quite difficult to read, which probably makes it easier to plant fakes than on the regular World Wide Web.

For example, the real and fake addresses for DuckDuckGo are the equally immemorable:

http://3g2upl4pq6kufc4m.onion/ (real)?http://3g2up5afx6n5miu4.onion/ (fake)
Nurmi also claims that the fake sites aren’t just duplicates of the real sites but proxies for them (he could presumably verify this for his own site but he doesn’t state how or if he tested it for the others).

If he’s correct then the proxies would allow the attacker to launch so-called Man-in-the-Middle attacks, stealing or modifying data as it passes through the fake site.

These sites are actually working as a transparent proxy to real sites. However, the attacker works as MITM [Man-in-the-Middle] and rewrites some content. It is possible that the attacker is gathering information, including user names and passwords.

In another sinister twist user ’garpamp’, who claims that such activity has been "going on for years", states that he’s seen pages that list .onion addresses being modified by malicious Tor exit nodes.

This is a completely different attack from the one identified by Nurmi and it occurs on the regular web, not the Dark Web, but it’s aimed at achieving the same thing - getting you to visit a fake Dark Web service instead of a real one.
It works like this:

The Tor browser can be used to browse hidden services on the so-called Dark Web, where both the browser and the site are completely anonymous, or the regular World Wide Web, where only the user with a Tor browser is anonymous.

When it’s used on the regular web, Tor encrypts your traffic and sends it on an eccentric journey between a number of Tor nodes before it’s decrypted again before making the final hop to its destination like any other internet traffic.

This decryption (and the encryption of responses) is performed by a special Tor node called an exit node. Anyone can set up an exit node and

because they deal with unencrypted information they are an excellent place to spy on traffic, or even to modify it on-the-wire (you can read more about exit nodes in my recent article Can you trust Tor’s exit nodes?).

What garpamp claims to have seen is malicious exit nodes being used to rewrite regular web pages.

In other words, if you looked at this page through Tor and you happened to get a malicious exit node in your circuit you might not see the legitimate DuckDuckGo address at the top of this page, you might see two fake ones instead.

During the course of the discussion, garpamp noticed that a bad exit node was actually rewriting the addresses on the pastebin page posted by Nurmi!

...I’ve also seen exits [1] rewriting onion addresses found on clearnet.

[1] Like the ****** behind this piece of **** is doing to that pastebin url... Arag0n 185.77.129.189 dc914d754b27e1a0f196330bec599bc9d640f30c

The thread closed with Roger Dingledine, one of the original Tor developers, reporting that the bad exit node discovered by garpamp has now been given the BadExit flag which should prevent it from acting as an exit node.

The battle to shut down bad exit nodes is ongoing.

We don’t know who is behind the fake sites, who is behind the exit nodes rewriting real addresses for fake ones or why they’re doing it, but there are no shortage of suspects.

The Dark Web is an online safe haven for dissidents, journalists and champions of free speech but it is also a small and highly concentrated den of the very worst criminality.

So, not only is there is an abundance of thieves on the Dark Web, and no honour amongst them, there is no shortage of government hackers or undercover agents either.

One Man Emailed 97,931 People To Tell Them Their Passwords Had Been Stolen

If you found a wallet lying in the street that contained thirty dollars and the owner’s address would you return it?

’Atechdad’ would.

Atechdad is the creator of the hacked site gallery urhack.com and he’s more familiar than most with the bits of the web where personally identifiable detritus washes up from so many internet break-ins.

He is, in his own words, somebody who runs "across lots of passwords on the webs".

What if someone returned your wallet, but cloned your credit card? You probably wouldn’t know anything was amiss. Losing a password is a bit like having your credit card cloned. Unlike losing your wallet, there isn’t a

particular moment when it’s no longer in your possession, only the moment where it’s no longer exclusively yours.

Which makes learning that your password has been stolen an unpleasant but necessary step in re-establishing the integrity of your privacy and security.

The web is, as Atechdad attests, littered with cloned passwords and yours might be among them.

To find out if they are, you’ll either have to conduct an exhaustive, never-ending search of the web’s grubby corners or pay somebody else to do it for you.

Assuming you even realise that such a service exists, and most of us probably don’t, you’ll have to decide if you trust it.

Atechdad had another idea:

I run across lots of passwords on the webs. Passwords to bank accounts, Netflix accounts, email accounts - you name it ... I wondered what would happen if I just emailed this information to the people who owned it.

So he set out searching Pastebin for credentials and after three days amassed a trove of nearly 98,000 email and password combinations.

And then he contacted all of them to tell them the bad news.

From: <canary urhack.com>
To: REDACTED
Cc:
Date: Tue. 19 May 2015 06:12:41 -0400
Subject: Your account may have been compromise&

To Whom It May Concern: An account associated with this email address may have been compromised. This email has been sent as a warning.

If these credentials match any you are familiar with. we recommend that you change your password as soon as possible. Otherwise. please disregard this message.

REDACTED

Why?

The scripts that urhack.com is powered by routinely come across sensitive information which has been published publically. This is usually the result of a hack. social engineering attack or phishing campaign. Many people may not know their accounts have been compromised. We send these emails as a service to let people know so they can take action.

About Canary

-urhack Canary

If you do not wish to receive these notifications in the future. please unsubscribe. We will not bug you again. Promise.

Those of you itching to know if this good Samaritan gesture was met with altruism in kind should prepare yourselves for disappointment; the

internet did not thank Atechdad.

It could have been the slightly spammy, lightly phishy nature of his communiquØ (note the typo in the subject line).

Or maybe, after years of disingenuous emails from rich Nigerian princes and beautiful Russian girls, we've lost faith in the claims of strangers.

Whatever the reason, Atechdad's 97,931 good intentions were just no match for the yawning, black hole of apathy and cynicism that our inboxes create.

Just 50 of the near-one hundred thousand recipients registered receipt of their email in any way whatsoever. Of those, 41 did so by unsubscribing themselves, leaving just nine (0.009% of people emailed) who felt his efforts warranted a thank you.

The evangelical are not easily dissuaded from their path by apathy or abuse though. Buoyed by what he describes as the success of his first trial, Atechdad has given his experiment a name, Robin, and vowed to do it again.

Microsoft Once Again Confuses Everyone About Who Gets Windows 10 for Free

Microsoft s Windows 10 OS might be one of the company s most important software releases yet. Not only is the Redmond-based giant looking to unify mobile, desktop and consoles with the help of new software, but Microsoft is also giving it away free of charge to many people who are using older versions of Windows only the company isn t always exactly sure who qualifies.

What s abundantly clear is that Windows 7 and Windows 8 home users will all get Windows 10 free of charge this summer when the OS launches. But on Friday, Microsoft made it sound like Windows XP and Vista users who registered for Windows 10 Insider access the company s beta program for Windows will be guaranteed free access to Windows 10 in the future.

Things quickly and silently changed over the weekend, Ars Technica points out. The company s blog post describing the Windows Insider preview program has been updated to reflect certain changes that Windows XP and Vista users will not appreciate.

The company initially said that members of the Insider program running a preview version of the operating system would receive the Windows 10 final release build and remain activated but then changed it to receive the Windows 10 final release build, which is practically the latest beta version that Insiders will get to use before the OS is launched.

 It s important to note that only people running Genuine Windows 7 or Windows 8.1 can upgrade to Windows 10 as part of the free upgrade offer, Microsoft also added to the post. The mention contradicts Microsoft s Gabe Aul tweet on Friday. The exec said that the upgraded preview copies would be genuine, implying that Windows pirates would also be able to take advantage of this loophole.

So what does this all mean?

Ars suggests that the shift is more aimed at corporations and organizations that are going to be charged for getting their machines upgraded to Windows 10 en masse and not to individuals who have pirated versions of old Windows versions. In other words, if you have a pirated copy of Windows, don t worry about Microsoft denying you access to free Windows 10 just yet.

=~=~=~=